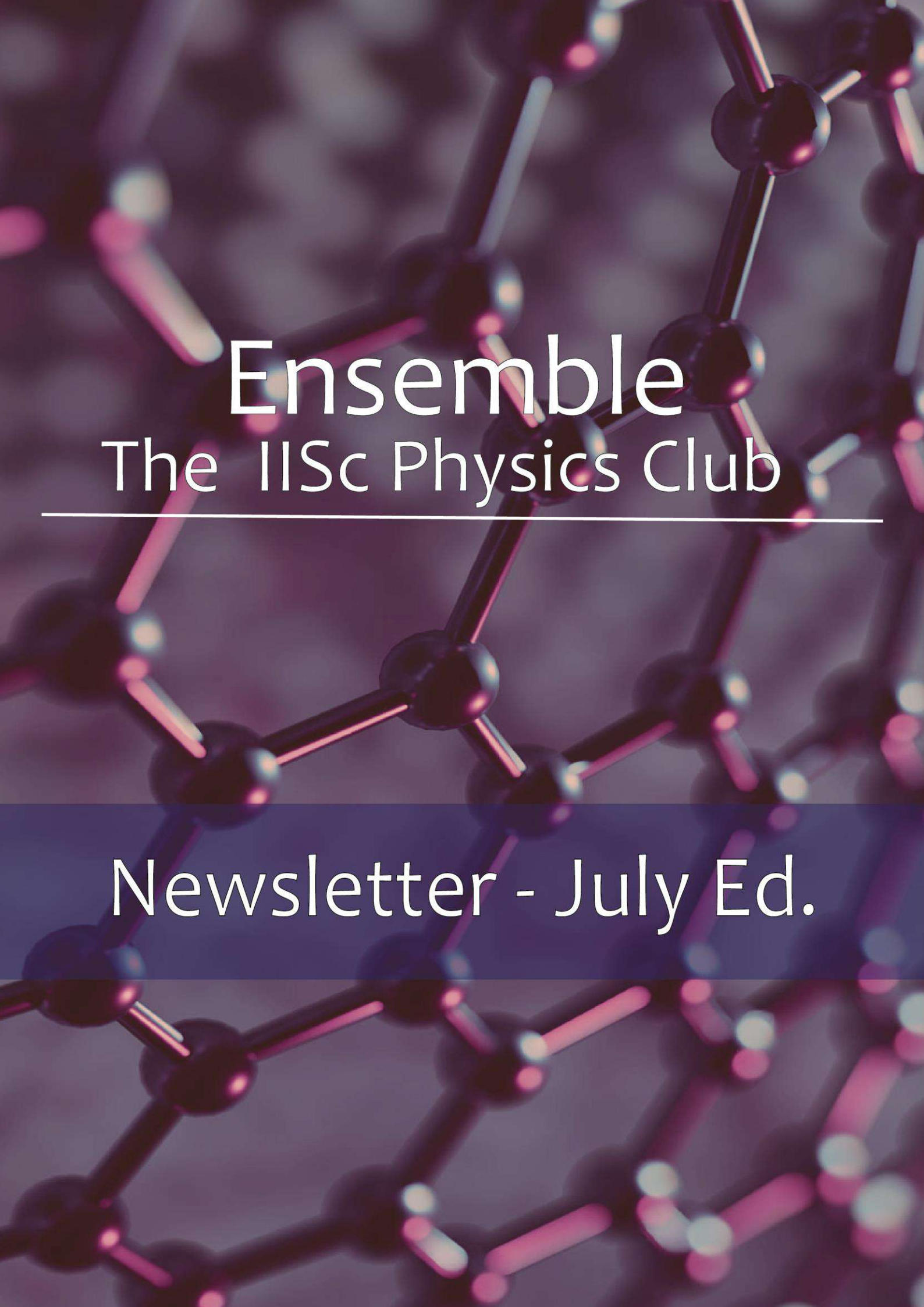


Ensemble

The IISc Physics Club

Newsletter - July Ed.

Implementation of Spin Qubits

Introduction

Spin qubits manipulate the spin of charge carriers in semiconductor devices, such as electrons and electron holes. Daniel Loss and David P. DiVincenzo proposed spin qubit computers in 1997, aiming to leverage the intrinsic spin 1/2 degree of freedom of individual electrons in quantum dots as qubits. Only when the phenomenon of Coulomb blockade was found, which enabled us to grow quantum dots in aluminum tunnel junctions at cryogenic temperatures, was this qubit experimentally realized. Using two or more layers of semiconductors, known as semiconductor heterostructures, to confine electrons to a two-dimensional plane is now one of the most popular methods for creating quantum dots. This process is known as a 2DEG (two-dimensional electron gas). A series of metal gates on the surface of the semiconductor control the energy of the quantum dot, a design referred to as the lateral gating quantum dot. In these quantum dots, the gate electrons have a quantized energy spectrum comparable to that of atoms.

There are numerous types of spin qubits based on quantum dots, but they all have a similar set of fundamental characteristics. Additional quantum dots add complexity by allowing for more control parameters and, in particular, by enabling the partial encoding of the qubit state in the location of the electrons within the quantum dots, giving them a dipole moment. Controllability, speed, and noise are only a few of the trade-offs between the various topologies and materials.

Implementation

Spin qubits can be categorized based on the quantity of quantum dots involved. Single Spin Qubits employ a single quantum dot, while Charge Qubits and Triple-dot Qubits employ multiple quantum dots. The first type typically just depends on the spin state, whereas the latter type may also depend on the spin's location, or charge state. Magnetic fields primarily control the first variety, while the ones in the second group are managed by shifting the electron between dots using voltages. This exposes it to charge noise, one of the main modes of decoherence in the system.

Single Spin Qubits

A single electron in a single quantum dot with the logical subspace consisting of |↑> and |↓> (the "up" and "down" spin states) is our concerned spin qubit. These can be controlled by using magnetic resonance techniques to perform electron spin resonance. Applying a static magnetic field to split the energies of the spin states and an oscillating magnetic field perpendicular to the static one at a frequency close to qubit splitting, drives oscillations around the Bloch sphere. We write the Hamiltonian of the system (taking static field along z direction and AC field in x direction) as:

$$H = g\mu_B(B_z\sigma_z + B_x\sigma_x cos(\omega t + \varphi))$$

Where ω is the AC frequency and φ is the phase of the AC signal. Making the rotating frame transformation for the resonant case, this comes out to be:

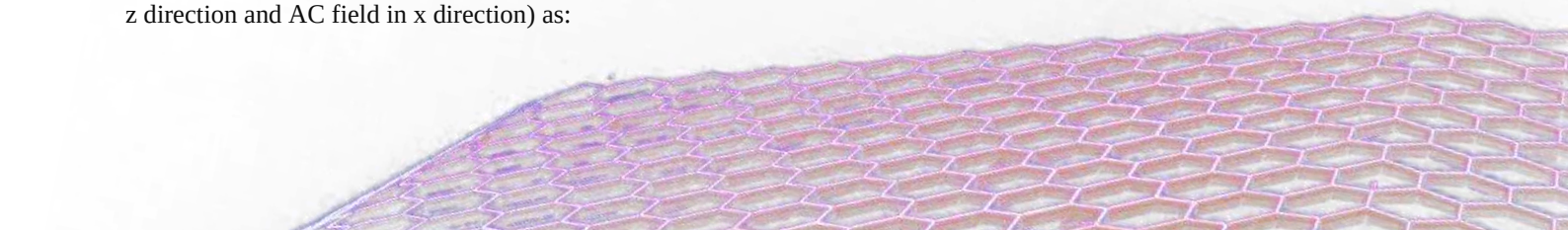
$$H_{rot} = g\mu_B(B_x cos(\varphi)\sigma_x + B_x sin(\varphi)\sigma_y)$$

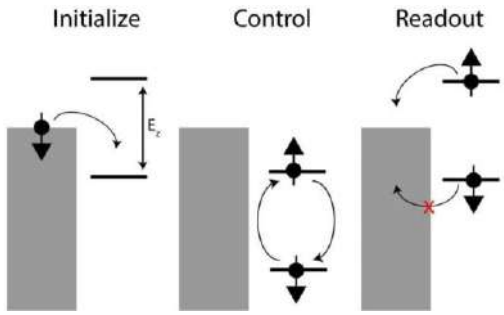
For general research reasons, all qubits are subjected to a static magnetic field of around 1T. The oscillating magnetic field (whose amplitude is typically significantly less than the static field) can be applied via various methods. Utilizing a coplanar waveguide (CPW) is one method. A CPW comprises two ground planes on either side of the center conductor, all of which are in the same plane and positioned above a dielectric block. It functions by focusing EM radiation inside the dielectric. However, because CPW has a vast special extent and requires high voltages to produce fast Rabi rates, which makes it challenging to address single qubits, it can generate a significant amount of heating.

Making a spin qubit involves loading the initial state, performing oscillations around the Bloch sphere and reading out the final state. This is achieved by using one high-frequency gate electrode per qubit. To load the qubit in a particular state, for example, in | ↓>, the gate electrode shifts the qubit energy to ensure that |↓> has a lower energy than the lead (in the quantum dot circuit) and |↑> is in a higher energy so tunnelling between dot and leads reset the qubit to |↓>. Next, the gate voltage is shifted to decouple electron from the lead and quantum gate operation is performed. Readout is performed by first performing the necessary rotation to measure the correct qubit orientation upon which the gate voltage is shifted in the same arrangement as the initialization. This ensures that electron can tunnel only if it is in the | ↓> state, which can be detected by a QPC.

Sillicon-Metal-Oxide-Semiconductor (Si-MOS) for quantum dots

This design involves an insulator deposited on silicon and depletion and accumulation gate electrodes are deposited on top of it. The silicon is undoped, so the accumulation and depletion gate voltages are adjusted to accumulate a 2DEG at the insulator-semiconductor interface to form quantum dots. The use of overlapping gates (fig1) in which gates are deposited in multiple overlapping layers with a thin insulating layer between them prevents shorting and helps define the quantum dot better. They possess an increased effective mass in these silicon systems than their analogue GaAs systems, which decreases the Fermi wavelength forcing the dots to be smaller.





The main challenge in silicon qubits is valley degeneracy. This arises because silicon has six degenerate energy valleys in its conduction band and electrons in quantum dots can be in any of them. To make them into functional qubits, the degeneracies must be lifted because small energy differences between the valleys can cause leakage out of the logical subspace and cause the relaxation time to be reduced. Confinement in the z direction shifts the energies of four of the states and the rest of the degeneracy can be lifted by application of electric fields through gating. The valley split value in such a technique can reach upto 0.8MeV.

This implementation has used co-planar waveguides to perform single qubit gates. Two qubit gates in the realm of this implementation have a fidelity of over 90%, Rabi rates in the order of hundreds of kHz, entanglement rates close to 1MHz and readout fidelities around 80-95%.

qubits, the degeneracies must be lifted because small energy differences between the valleys can cause leakage out of the logical subspace and cause the relaxation time to be reduced. Confinement in the z direction shifts the energies of four of the states and the rest of the degeneracy can be lifted by application of electric fields through gating. The valley split value in such a technique can reach upto 0.8MeV.

This implementation has used co-planar waveguides to perform single qubit gates. Two qubit gates in the realm of this implementation have a fidelity of over 90%, Rabi rates in the order of hundreds of kHz, entanglement rates close to 1MHz and readout fidelities around 80-95%.

Si/SiGe systems

This system uses a quantum well of silicon, approximately 10nm thick, between layers of $Si_{1-x}Ge_x$, where x is approximately 0.3. There are many similarities between Si/SiGe systems and Si-MOS systems as both are gate-defined quantum dots whose wavefunction is primary in silicon. Both stadium style and overlapping gates have been used for these devices. While some devices use doping to populate the 2DEG, it is more common practice to use undoped silicon. Micromagnets are used for single qubit gates over CPW in the transmission part. The valley degeneracy in Si/SiGe is lifted by strain between the Si and the SiGe as well as vertical confinement and small valley splittings are lifted by adjusting local gate voltages.

Using natural silicon and micromagnets, gate fidelities reach 99% and Rabi rates are approximately 1MHz. Readout fidelities of 70-85% are achieved.

Donors

They are single atoms situated in a semiconductor and possessing bound hydrogen-like states. For example, a phosphorous atom in silicon has a bound electron and nuclear spin, both of spin ½ allowing us to use both of them as qubits. The donors are formed either through ion implementation or by positioning them using lithography with a Scanning Tunelling Microscope, which offers the possibility of precise placement for multiple qubit systems. In donor-based systems, the gate electrodes are not needed to define the quantum dot potential and are needed only for performing quantum gate operations. The electron state has a Bohr radius of about 2mm, which becomes important in exchange-based operations (as the two QD's need to be extremely close to each other to allow for non-zero tunnelling).

To perform initialization and readout, a single-electron transistor is fabricated adjacent to the donor qubit which acts as both a lead and the sensor. Readout fidelities are observed over 97%. Measurements of electron qubit in ion-implanted single donors in isotopically-purified silicon have shown high coherence times.

Two qubit gates between donor electrons rely on the exchange interaction, but this poses challenges as donors need to be extremely close together owing to their narrow wavefunctions. For STM-placed donors, it is easier to design specific exchange couplings, but there are still challenges such as exchange coupling's oscillation in magnitude with donor separation owing to valley interference. Exchange rates have been measured with speeds approaching 1GHz.

Charge Qubits

These have one electron in a Double Quantum Dot with a representing Hamiltonian H= $\varepsilon/2\sigma_z + t_c\sigma_x$, with a logical subspace that entails the electron being in the right or left dot. The distribution in the qubit can be changed by changing the voltage detuning ε between the dots. When ε is large and positive, the align with electron being in right and left QD and $H \approx \varepsilon\sigma_z$ and vice versa for negative ε. At $\varepsilon = 0$, the left and right states are degenerate and $H \approx t_c\sigma_x$. Charge qubits can be hence controlled by gate voltages alone without application of resonant pulses. The qubit's splitting changes magnitude and relative amounts of σ_x and σ_z with changes in local voltage which corresponds to rotation and length change in Bloch sphere representation. Also, these charge qubits are highly coupled to charge noise, stemming from fluctuations in the environment leading to decoherence. Thus, their use in quantum computers and other technologies have been limited.

Triple dot Qubits

Recent developments suggest a three dot, three electron system, forming a triple-dot or exchange-only qubit. These

qubits utilize the exchange between the left and middle dot and the right and the middle dot, allowing us two independent axes of control. These qubits thus have charge states in (2,0,1), (1,1,1) and (1,0,2) configurations giving a logical subspace of

a singlet-like ground state and a triplet-like excited state. The Hamiltonian can be controlled with detuning between the left and the right quantum dots. Initial experiments were performed in GaAs/AlGaAs and were limited by magnetic-field noise. More recently, they have been studied in isotopically purified Si/SiGe. Experiments showed an average error of 0.3% with half the errors stemming from leakage.

Sources and challenges

The number of coherent operations that can be performed by a quantum computer is ultimately limited by the decoherence of the quantum system. They generally stem from magnetic noise and charge noise.

In GaAs/AlGaAs heterostructures, the nuclei of Al, Ga and As all have nuclear spin I = 5/2, which generate an effective magnetic field that acts on the qubit. The noise arising from this nuclear bath makes it difficult to establish coherence in GaAs/AlGaAs qubits. The other major source of noise comes from fluctuating charges near the qubit. It is hypothesized to have stemmed from charge traps near the surface or in the oxide layers for qubits that possess one. In most charge-like qubits, the sensitivity to charge noise, which is given by the derivative of the splitting with respect to detuning voltage, is voltage dependent. This makes quantifying the error trickier than the case of nuclear noise.

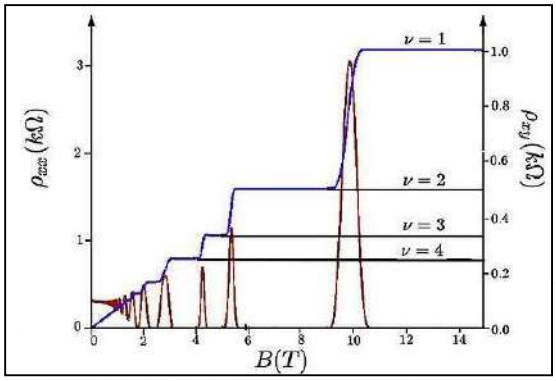
Review - Quantum Spin Hall effect

Abstract

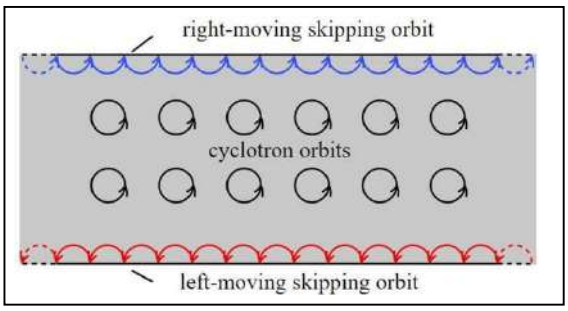
The quantum spin hall effect(QSHE) was first proposed by C. Kane and G. Mele. in 2005 in a graphene which is based on the model of D. Haldane which was proposed in 1988. In the normal version, it was predicted that if a current is passed through a 2d material, then there will be an accumulation of different spin of electrons on the opposite sides of the material. Whereas in QSHE, there are currents on the edges of the material having different directions based on the electron spin. In the QSHE and SHE, there is no need for a magnetic field. The origin of the effectis spin-orbital coupling. The QSHE was first experimentally shown in 2007 by S. Zhang, not in Graphene but in mercury telluride (HgTe) wells because of higher spin orbital coupling. QSHE is shown by the topological insulators that are insulators in the bulk and hence have a band gap therebut are conductive are the surfaces hence a gapless state. The edge state in QSHE is also time reversal invariant which is not in the case of QHE or SHE.

Quantum Hall Effect

Quantum Hall effect is the quantized version of the Hall effect. Here is a 2D material at a low temperature, the transverse conductance is quantized and equal to $\frac{\nu e^2}{\hbar}$ where

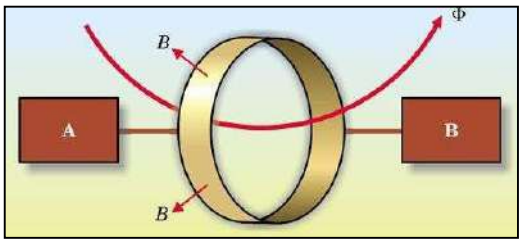


ν is filling factor of landau levels(quantized energy levels of electrons in the magnetic field), and hence formplateaus in the Rxy vs B graph. The plateaus are topologically robust, and their flatness is nearly independent of the impurities of the material. This effect was first discovered by K. von Klitzing in 1980. It was realized that the current is carried by edge states instead of the bulk of the material which become insulating.



Laughlin Argument and topological aspects

The robustness of the plateaus were explained by Laughlin in 1980. In his argument, he constructed a hypothetical conducting ribbon with a radial and an axial magnetic field and two electron reservoirs at the ends A and B. The axial flux is increasing very slowly, which produces an emf along the circumference. By classical theory, electrons should be following from reservoirA to B, and according to Aharonov -Bohm effect, the system should be gauge invariant where theflux changes by one flux



quantum, that is h/e. Therefore there is a shift of electrons in the landau levels and the system maps back to itself. The current along circumference is given by $\frac{\nu e^2}{\hbar}$ and $\Delta E = \nu eV$, where ν is the number of filled Landau levels and V is the potential difference of two sides and the conductance turns out to be $\frac{\nu e^2}{\hbar}$. Hence the robustness comes from the gauge invariance. The gauge invariance is related to the Berry phase. It was shown by Thouless, Kohmoto, Nightingale and den Nijs, that the landau filling number is exactly equal to the Chern number in

$$n = \sum_m \frac{1}{2\pi} \int_0^{\Phi_0} d\,\Phi \int dk_x F\left(k_x, k_y^m(\Phi)\right)$$

k-space And the chern number is invariant for a surface with smooth deformation, hence a reason forrobustness.

Haldane Model

Haldane started with a graphene layer and considered electrons to be spinless. Graphene has a really nice band structure and is conductive as there is a conductive band and valence band touching at 2 points in the Brillouin zone, and the points are called Dirac Points. Haldane started with the argument that if

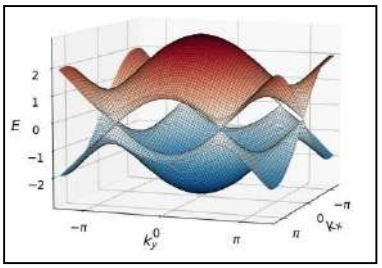
inversion symmetry or time symmetry is broken, then there would be a band opening at Dirac points

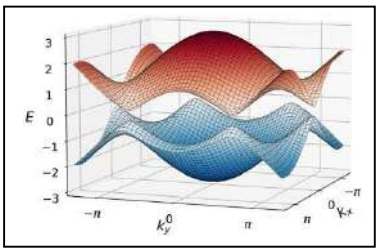
The Hamiltonian of graphene is given by

$$H = \begin{pmatrix} M & t_1 \sum e^{-ik.a_i} \\ t_1 \sum e^{ik.a_i} & -M \end{pmatrix}$$

$$= t_1 \left(\sum cos(k.a_i) \right) \sigma_x + t_1 \left(\sum sin(k.a_1) \right) \sigma_y + M\sigma_z$$

Where t_1 is the nearest neighbour hooping parameter and a_i are the lattice vectors and M is the onsite Energy of the K point





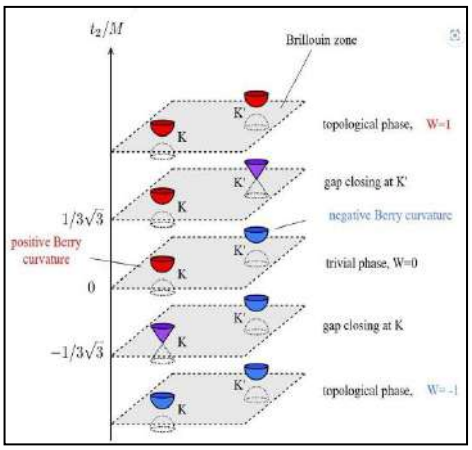
He introduces a second nearest neighbour hooping parameter which is complex which results inthe breaking down of time reversal symmetry and the Hamiltonian become

$$H = \begin{pmatrix} t_2 \sum (e^{i\varphi} e^{-ik.b_i} + e^{-i\varphi} e^{ik.b_i}) + M & t_1 \sum e^{-ik.a_i} \\ t_1 \sum e^{ik.a_i} & t_2 \sum (e^{-i\varphi} e^{-ik.b_i} + e^{i\varphi} e^{ik.b_i}) - M \end{pmatrix}$$

$$= t_1 \left(\sum cos(k.a_1) \right) \sigma_x + t_1 \left(\sum sin(k.a) \right) \sigma_y$$
$$+ 2t_2 \cos\varphi \left(\sum cos(k.b_i) \right) I + \left(M - 2t_2 \sin\varphi \left(\sum sin(k.b_i) \right) \right) \sigma_z$$

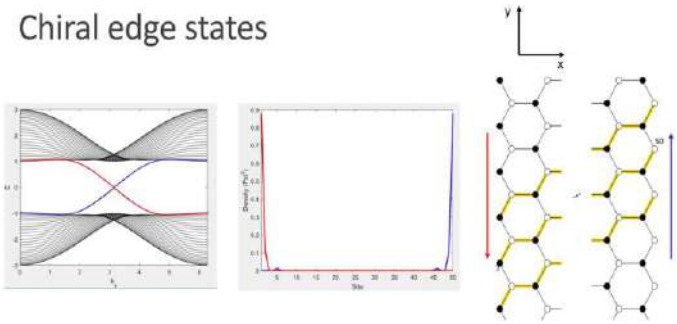
Where second order hooping parameter is $t_2 e^{i\varphi}$ and b_i be the vector for next nearest lattice vector.Haldane showed that based on the value of t_2 and φ graphene goes through the transition where its chern number changes.

The above illustration is for the $\varphi = \pi/2$ hence the second nearest hooping parameter is purely complex. When $|t_2/M| < 1/3\sqrt{3}$ then the graphene is a trivial insulator and the chern number is 0 on average. But when the value in become equal, i.e., $|t_2/M| = 1/3\sqrt{3}$ then one of the Dirac points touch each and there is flip of the berry curvature and hence the chern number becomes ± 1 and the graphene become topological



insulator. And there will be conducting edge state with only movement along one dimension.

And again here the invariance of chern number is responsible for the robustness of the edge states.



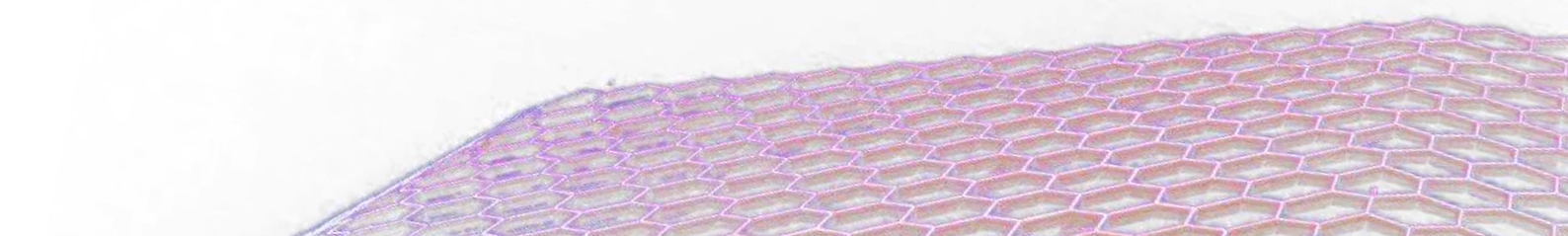
Kane and Mele model and QSHE for graphene

In Kane and Mele model they added to spin term to the Haldane model and they took copiesof it, in order to make the whole Hamiltonian time reversal invariant. They included the spin orbital coupling term into the Hamiltonian. And the net Hamiltonian become

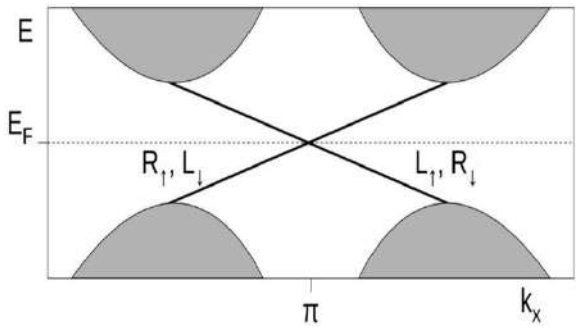
$$H = t_1 \left(\sum cos(k.a_1) \right) \sigma_x + t_1 \left(\sum sin(k.a) \right) \sigma_y + \left(-t_{SO} \left(\sum sin(k.b_i) \right) \right) \sigma_z s_3$$

Where s_3 it the third spin matrix. The energy eigenvalues are given by

$$E_{\pm}(k) = \pm \sqrt{t^2 \left(3 + 2 \sum cos(k.b_i) \right) + 4t_{SO}^2 \left(\sum sin(k.b_i) \right)^2}$$



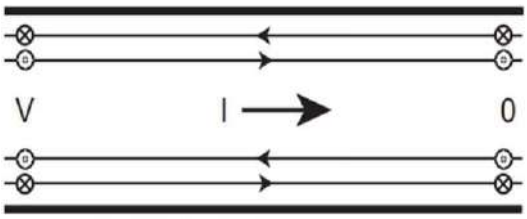
It has been shown that at in the bulk there is band gap whereas the edge states are gapless. The E-k diagram will be like as follows.



Here the opposite edge states have spin polarized, i.e., of opposite spin hence combining the two copies we get edge states in both the degree of freedom.

And both states give quantum hall effect with spin dependent chirality.

Hence to total number of degree of freedom is 4, 2 on the upper edge and 2 on the lower edge.These edge states are protected by both time reversal symmetry as well as the inversion symmetry



QUANTUM SAFE CRYPTOGRAPHY: A REVIEW

Cryptography ensures that messages or information passed between parties are authentic (the receiving party knows that the correct sending party gives the message) and confidential (basically, no eavesdropping allowed!). A pretty standard scenario in this regime is depicted by two parties, Alice and Bob, who are communicating over some channel, and there is an adversary Eve who wishes to either gain information about the messages (other than length), change, or corrupt the message. The idea is to develop systems that prevent such things from happening (you wouldn't like the chats between you and your "significant other" on WhatsApp to be leaked by a third party, would you? That's one example where WhatsApp's cryptographic encryption methods help!). Now you may ask, "Wait a minute, this is being done on classical systems! Where's the 'quantum' part?". Well, the quantum part can be understood in two ways here:

1. Either the ideas of Quantum physics are used to build such cryptosystems (Quantum Key Distribution, Quantum Money, etc.)
2. Quantum algorithms are used to attack our current cryptosystems, creating the need for modified schemes to withstand such attacks. This comes under **Post-Quantum Cryptosystems.**

A general idea in building such cryptosystems is centering the protocol around an existing **hard** problem (no, your math homework in 12th grade doesn't come under this definition). A hard problem here generally refers to a problem that currently doesn't have any algorithm which solves it in polynomial running time (say a problem is characterized by some length parameter n, then a polynomial time algorithm is of the form of $f(n)$, where f is a polynomial on variable n). In complexity theory comes under the branch of **NP** (solution can be guessed non-deterministically and verified in polynomial time).

I'll demonstrate this with a classic system known as **RSA** (Rivest-Shamir-Adleman) signature scheme. Before that, we have to understand a digital signature scheme. It is a protocol consisting of three parts: **Key-Gen** algorithm, **Signing** scheme, and **Verifying** scheme. The Key-Gen algorithm creates two objects (generally bit strings composed of 0's and 1's), a **public key** (pk) which is shared with everyone, and a **secret key** (sk) known only to the party that runs the algorithm. When the party has a message to share with another party, it firsts runs key-gen and gets the <pk,sk>.

The signature scheme takes in the arguments of the message (m) and sk and outputs a signature (σ):

$$\text{Sign}(m, sk) = \sigma$$

This signature is then sent along with the message to the other party. The other party then runs the verification algorithm to check if the signature is of the same message or not (as it could have been tampered with by the adversary!):

$$\text{Verify}(m,pk,\sigma) = 0 \text{ (rejects) or } 1\text{(accepts)}$$

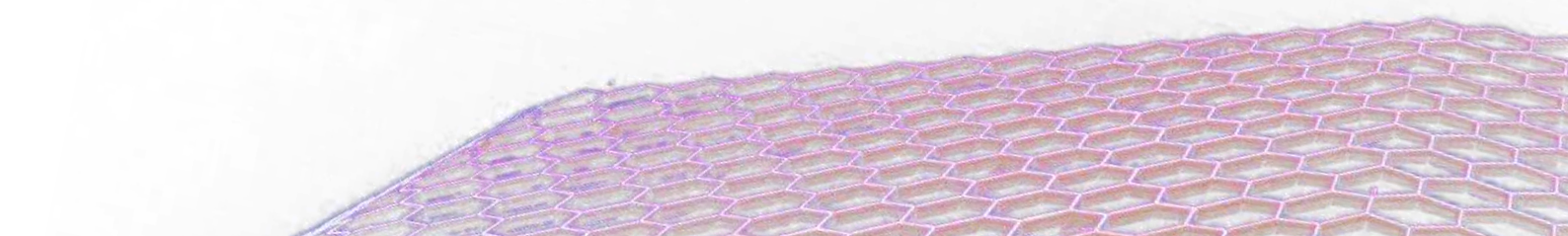
A secure scheme here must ensure that a probabilistic-polynomial-time (**PPT**) adversary is not able to come up with a "new" message-signature pair (m^*,σ^*) (different from the previous ones used in the communication channel) that is verified successfully by the receiving party, as it would mean that the adversary has created a forgery. With these ideas in mind, here is the RSA scheme:

- **Key-Gen:** Chose two *large* primes p and q.
  - Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
  - Randomly choose an odd number e that is co-prime to $\phi(n)$.
  - Compute d s.t. $ed \equiv 1 \bmod \phi(n)$.
  - Pick a "cryptographic" hash function $H : \{0,1\}^* \to [1, n-1]$.
  - Public key: (e, n, H); secret signing key: d.
- **Sign:** Given a message $m \in \{0,1\}^*$ compute $H(m)$ and the signature $\sigma = H(m)^d \bmod n$.
- **Verify:** Given (m, σ) compute $H(m)$ and $\sigma^e \bmod n$. Accept σ as a valid signature on m if and only if $H(m) = \sigma^e \bmod n$.

What is a **Hash function** here? Hashing refers to the idea of taking a string of arbitrary length and mapping it to some other string of a fixed length in a **pseudorandom** way that does not disclose any information about the original string (essentially a method of encryption). The $\{0,1\}^*$ here means a bit-string of arbitrary length, and H is the hash function acting on this domain.

As we can see here, we do not want the adversary to know the secret signing key d, as it would allow them to create forgeries. The adversary can do this by either finding the prime factors of n, which are p and q (Integer factorization) or by computing $H(m)$ and then using the signature relation $\sigma = H(m)^d \bmod (n)$ to obtain d (similar to the **Discrete logarithm problem**, but not quite the same). However, both issues are

fortunately 'hard' for any PPT bounded adversary! Hence this forms a secure cryptosystem….or does it?



Discrete Log Problem (DLP):

- Instance: A cyclic group $\mathbb{G} = \langle g \rangle$ of prime-order p and an element $h \in \mathbb{G}$.
- Task: Compute $a \in \mathbb{Z}_p$ such that $h = g^a$.

Peter Shor's *quantum* algorithm attacks this tough **Integer factorization problem** (and DLP as well) and solves it exponentially faster than our current classical algorithms on a quantum computer. And the most significant number that has been factorized by Shor's Algorithm up until now is… (*wait for it)*... 21 = 7×3 (wow, what a bummer, we were getting worried for nothing after all!).

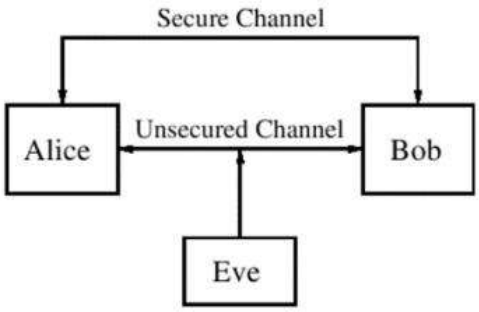
Quantum Algorithm

- 1985: David Deutsch developed the idea of Quantum Turing Machine.
  - Asked whether quantum computers can be useful for classical problems.
  - Showed a single query suffices to decide whether a one-bit function is constant or balanced.
- 1994: Peter Shor proposed a quantum algorithm for factorisation in polynomial time. Solves DLP as well.
- 1997: Lov Grover developed a quantum search algorithm with $\approx \sqrt{N}$ complexity, where N is the size of the unsorted database.
  - AES-128 key can be recovered in $\approx 2^{64}$ operations.

Well, Shor's algorithm hasn't led to any practical jailbreaks for the RSA system yet, but that's the engineers' fault (no shade thrown, these people are trying their very best!) The theoretical arguments are pretty sound, and thinking about cryptosystems that can deal with such threats effectively becomes necessary. To that end, several schemes have been made, which are listed below:

1. Information-Theoretic Security: One-Time Pad (1882).
2. Symmetric-key Cryptography: Advanced Encryption Standard or AES (1998).
3. Hash-Based Cryptography: Merkle's hash-tree Public Key Signature (1979).
4. Multivariate-Quadratic Based Cryptography: Patarin's Signature Scheme (1996).
5. Code-Based Cryptography: McEliece's Public Key Encryption (1978) based on Hidden-Goppa-Code.
6. Lattice-Based Cryptography: "NTRU" PKE by Hoffstein, Pipher and Silverman (1998).
7. Isogeny-Based Cryptography: Supersingular Isogeny Diffie-Hellman Key Exchange by Feo, Jao and Plut (2011).

What I have been discussing until now Comes under the **Public-Key Cryptography** (PKC) class mainly. Another broad class is **Symmetric-Key Cryptography** (SKC), where the communicating parties already have a shared secret key k between them and an encryption (and decryption) scheme to send messages. Generally, a hybrid model is followed where a PKC scheme like Diffie-Hellman Key exchange is used to authentically share the secret key k (of some SKC) between both parties. Then encrypted messages are sent over the communication channel.



The topics in this Issue were written by the 2023 Ensemble Club convenors (from left to right):

Debadrito Roy (Implementation of spin qubits in real life), Aman Goyal (Quantum Spin Hall effect), and Soumyadeep Sarma (Quantum Safe Cryptography), as a special edition on Quantum-based applications!

Hope you enjoyed this July issue of the Ensemble Newsletter! For more information about what we do, or to subscribe to our mailing list, where we share information about our events and newsletter, go to our website!